III. CLAIM AMENDMENTS

1. (Currently Amended) A method for establishing and managing a trust model between an identification module and a radio terminal, said method comprising~~characterized in that it comprises~~:

authenticating a radio terminal ~~authentication step~~ by said identification module, said ~~identification step~~ authenticating ~~authentication~~ being carried out by ~~means of identification~~ radio terminal authentication means that are provided either to said identification module by a mobile radio-telephony network at the time of an initialization ~~step or similar~~ or at the time of an ~~a so-called~~ updating ~~step~~, or to said radio terminal by the identification module; and

~~a control step~~ controlling by said identification module ~~of~~ at least one specific characteristic of the radio terminal, said specific characteristic being previously transmitted by radio-telephony to said identification module from a secured server of said mobile radio-telephony network.

2. (Currently Amended) The method according to claim 1, wherein ~~the lifetime of~~ said radio terminal authentication means present in the identification module are provided with a validity period that is limited by a determined expiration date, said authentication means being comprised of at least one authentication key.

3. (Currently Amended) The method according to claim 1, wherein said identification module comprises at least one of~~is~~ an SIM type chip card, ~~or~~ an USIM card for third-generation networks, or an equivalent card comprising in a memory the representative subscription data.

4. (Original) The method according to claim 1, wherein the identification module maintains a trust relationship with the radio terminal by generating authentication means and then by providing these authentication means to the radio terminal by

secured exchange mechanisms based on authentication means initially available from the radio terminal.

5. (Currently Amended) The method according to claim 1, comprising at the time of said initialization or updating generating ~~step a generation step~~, carried out at least by said identification module, ~~of a so called~~ trust key, said trust key being used by said module for encrypting at least data exchanged between the identification module and the radio terminal.

6. (Currently Amended) The method according to claim 2, wherein said initialization ~~step~~ of said authentication means is done on the initiative of the radio-telephony network, after denial of the key initiated by at least one of said module, ~~or~~ the mobile radio-telephony network, or the radio terminal, following an expiration of the validity period of the key or ~~even~~ at the time of initialization of the identification module.

7. (Currently Amended) The method according to claim 1, wherein said ~~authentication~~ authenticating~~step~~ comprises ~~especially the following steps~~:

~~an~~ utilization ~~step~~ in the radio terminal of at least one first authentication key memorized in the radio terminal by at least on first authentication algorithm memorized in the radio terminal, said first key having a validity period limited by a predefined expiration date;

~~an~~ utilization ~~step~~ by the identification module ~~of utilization~~ of at least one second key memorized in the identification module by at least one second authentication algorithm memorized in the identification module, said second key being identical or complementary to the first key and associated with the radio terminal, said second key having a validity period limited by said predefined expiration date; and

~~a comparison step~~ comparing in the identification module ~~for comparing~~ the results obtained by said first and second authentication algorithms.

8. (Currently Amended) The method according to claim 2, wherein ~~the~~ said authenticating ~~authentication step~~ comprises the utilization of said predefined expiration date.

9. (Currently Amended) The method according to claim 7, wherein said initialization ~~step~~ is initiated by a mobile radio-telephony network and also comprises:

generation by the identification module of at least one of said first and second keys;

~~a~~ storage in the identification module of said second key; and

transmission to the radio terminal by the identification module of said first key, said first key being encrypted by use of the trust key.

10. (Currently Amended) The method according to of claim 7, wherein said comparing ~~comparison step~~ is done between~~, on the one hand,~~ a response produced by said first authentication algorithm, stored in memory in the radio terminal and transmitted to said identification module and~~, on the other hand,~~ a response result, stored in memory in the identification module, produced by said second authentication algorithm.

11. (Original) The method according to claim 7, wherein said first key is an asymmetrical private key Ks and said second key being a public key Kp complementary to the first key.

12. (Original) The method according to claim 7, wherein said first key is symmetrical, said second key is stored in memory in the identification module being identical to the first key, these keys forming a single symmetrical authentication key.

13. (Currently Amended) The method according to claim 7, further comprising ~~an~~ updating ~~step~~ of said first and second keys, initiated by the identification module prior to said predefined expiration date, said updating ~~step~~ including ~~the following substeps~~:

authentication between the radio terminal and the identification module using said first and second keys;

generation by an updating algorithm of the identification module of at least one updated key taking into account ~~an~~ information for replacing at least one of said first and second keys;

memorization in the identification module of the updated key for replacing said second key; and

transmission to the radio terminal by the identification module of the updated key analogue of said first key.

14. (Currently Amended) The method according to claim 13, wherein said updating ~~step~~ further comprises ~~in addition~~ the control of at least one of one identifier of the radio terminal ~~and/~~or of the identification module.

15. (Currently Amended) The method according to claim 13, wherein an encryption of the key is carried out for said transmission to the radio terminal of the updated key analogue of the first key, said key encryption being done by said trust key.

16. (Currently Amended) The method according to claim 13, wherein the updating ~~step~~ also comprises ~~the following steps~~:

generation by the identification module of a new trust key after said authentication between radio terminal and module;

memorization in the identification module of the new trust key;

transmission to the radio terminal by the identification module of the newly generated trust key.

17. (Currently Amended) The method according to claim 13, wherein said updating ~~step~~ is completed by a verification test comprising a return transmission on the part of the radio terminal of at least one datum representative of effective receipt of data transmitted by the identification module during the updating ~~step~~.

18. (Currently Amended) The method according to claim 5, wherein said trust key is a symmetrical encryption/decryption key analogous ~~or identical~~ to said symmetrical authentication key.

19. (Original) The method according to claim 5, wherein said trust key is an erasable session key.

20. (Currently Amended) The method according to claim 7, wherein a ~~so-called~~ revocation ~~step~~ is carried out on the initiative of the identification module, of the radio terminal, or of the corresponding radio-telephony network, said revocation ~~step~~ comprising the erasure in a memory of said identification module of at least said first key associated with the radio terminal.

21. (Currently Amended) An identification module in a radio terminal ~~for the implementation of the method according to claim 1, charecterized in that it comprises means~~ comprising a device for memorizing at least one authentication algorithm, a calculation device ~~means~~ for executing at least ~~one step consisting of~~ applying an~~said~~ authentication key to said authentication algorithm as well as at least one authentication algorithm memorized in the identification module, a communication ~~device~~device~~means~~, ~~means~~a device for initiating a revocation and a revocation device ~~means~~ for revoking said authentication key, ~~means~~ a device for memorizing a specific characteristic of the radio terminal and ~~means~~ a device for actuating an updating algorithm for updating said authentication key, the communication ~~means~~ device being capable of providing at least one authentication key to the radio terminal and receiving data send from a secured server of a mobile radio-telephony network.

22. (New) The method according to claim 5, wherein said trust key is a symmetrical encryption/decryption key identical to said symmetrical authentication key.